Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/050829

International filing date: 25 February 2005 (25.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0401976
Filing date: 27 February 2004 (27.02.2004)

Date of receipt at the International Bureau: 23 June 2005 (23.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 01 JUIN 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg - 75800 Paris Cedex 08

Pour vous informer : INPI DIRECT
INPI Indigo 0 825 83 85 87
0,15 € TTC/mn
Télécopie : 33 (0)1 53 04 52 65

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

verifié
N° 11354*03

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 @ W / 030103

Réservé à l'INPI

REMISE DES PIÈCES
DATE 27 FEV 2004
LIEU 54 INPI NANCY

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0401976

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 27 FEV. 2004

Vos références pour ce dossier *(facultatif)* 017096

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
9 rue Claude Chappe
57070 METZ
France

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de production d'un certificat numérique, certificat numérique associé, et procédé d'utilisation d'un tel certificat numérique.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☐ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		GEMPLUS
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	Avenue du Pic de Bertagne Parc d'Activités de Gemenos
	Code postal et ville	13420 GEMENOS
	Pays	France
Nationalité		française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 27 FEV 2004
LIEU 54 INPI NANCY
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0401976

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		LECLAIRE
Prénom		Jean-Louis
Cabinet ou Société		CABINET BALLOT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	9 rue Claude Chappe
	Code postal et ville	57070 METZ
	Pays	France
N° de téléphone *(facultatif)*		03 87 74 81 36
N° de télécopie *(facultatif)*		03 87 36 26 76
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
LECLAIRE Jean-Louis 93.4009

VISA DE LA PRÉFECTURE OU DE L'INPI
Christine HUGUIN

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE DE PRODUCTION D'UN CERTIFICAT NUMERIQUE, ET CERTIFICAT NUMERIQUE ASSOCIE, ET PROCEDE D'UTILISATION D'UN TEL CERTIFICAT NUMERIQUE

Dans le domaine des transactions électroniques sécurisées, l'invention concerne plus particulièrement la production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble des données pour produire un certificat numérique.

Par transaction électronique, on entend ici une transmission d'un ensemble de données numériques (ensemble qu'on appellera message ou message électronique par souci de simplicité) dans le sens le plus large. Il peut s'agir par exemple de la transmission d'un acte d'achat ou de vente, de la transmission d'une demande d'accès à un service en ligne, de la transmission d'un message d'information signé électroniquement, etc.

De telles transactions peuvent être sécurisées par l'utilisation d'algorithmes de chiffrement et / ou de signature (par exemple l'algorithme RSA) à clés asymétriques : une clé privée et une clé publique.

La clé privée est utilisée par l'émetteur pour signer un message avant envoi. La clé privée est une caractéristique de la personne qui émet un message signé, elle est conservée secrète, par exemple dans une mémoire d'un matériel propriété de l'émetteur du message. La clé privée peut ainsi être conservée sur un disque interne

d'un ordinateur personnel, dans une mémoire d'une carte SIM (Subscriber Identification Module ou module d'identification d'abonnés) d'un téléphone portable, dans une mémoire d'une carte à mémoire ou d'une carte à microprocesseur accessible en lecture par un ordinateur personnel par l'intermédiaire d'un lecteur de carte, etc.

La clé publique est utilisée par la personne qui reçoit le message, pour vérifier l'authenticité du message signé reçu et l'identité de l'émetteur du message reçu.

L'utilisation d'algorithmes de signature suppose, préalablement à toute transaction, que l'émetteur communique sa clé publique à la personne destinataire de la transaction. Cette communication peut être directe : envoi d'un message contenant la clé, envoi d'un support physique tel qu'une mémoire ou un disque sur lequel est mémorisée la clé, etc. Cette communication peut se faire également par l'intermédiaire d'une infrastructure de clé publique (ou PKI pour Public Key Infrastructure en anglais) ou infrastructure de certification.

Une infrastructure de clé publique fait intervenir notamment une entité de certification et un tiers certificateur, pour permettre une cohérence dans la gestion des couples de clés.

L'entité de certification est un organisme normatif qui définit notamment les conditions de certification, les données devant être incluses dans un certificat et la manière dont sont utilisés les certificats produits. De manière connue, un certificat comprend une clé publique et des données identifiant un ou plusieurs propriétaires de la dite clé publique et de la clé privée associée.

Le mot propriétaire doit être ici compris au sens large.

Le propriétaire des clés peut bien sûr être une personne physique. Mais le propriétaire peut également être un matériel auquel est attachée le couple de clé. Par exemple, dans une société de grande taille, propriétaire de plusieurs serveurs de transmissions de données numériques, il est fréquent qu'un ou plusieurs serveurs "possèdent" leurs propres clés.

Aussi, et selon les consignes de l'entité de certification, les données identifiant chaque propriétaire peuvent comprendre le nom de l'utilisateur et / ou son adresse postale et / ou ses coordonnées bancaires et / ou des numéros de carte d'identité et / ou des références identifiant un matériel propriétaire.

Un des formats de certificat couramment utilisé est le format X509, défini selon la norme Information technology - Open Systems Interconnection - The Directory : Public-Key and attribute certificate frameworks datée de Mars 2002 de l'International Telecomunication Union. Le format X509 comprenant, pour chaque certificat, les paramètres suivants :

- un numéro de référence associé au certificat
- une indication du procédé utilisé pour la signature numérique d'un message,
- les coordonnées de l'émetteur du certificat,
- la période de validité du certificat,
- les coordonnées du propriétaire de la clé
- la clé publique
- un ensemble de N champs libres d'utilisation
- la signature de l'émetteur du certificat

Le tiers certificateur émet les certificats numériques et les met à disposition du public pour consultation dans une base de données regroupant un ensemble de certificats. Le tiers certificateur est ainsi chargé dans

un premier temps de collecter et vérifier les informations devant figurer dans un certificat. Dans un deuxième temps, le tiers certificateur regroupe la clé publique et les données identifiant le propriétaire de la dite clé publique dans un message numérique qu'il signe avec sa propre clé privée pour former le certificat numérique. Enfin, le tiers certificateur met le certificat à disposition dans une base de données.

En consultant la base de certificats, et si elle fait confiance au tiers certificateur, une personne va pouvoir authentifier l'émetteur d'un message signé qu'elle a reçu ou chiffrer un message à sa destination, avant de valider ou non une vente, d'autoriser ou non l'accès à un site réservé aux abonnés, etc.

Les techniques de production et de mise à disposition de certificats numériques sont aujourd'hui assez répandues. Elles ont permis de sécuriser dans une certaine mesure les transactions électroniques pour permettre leur développement. L'intervention d'un tiers certificateur, l'utilisation d'algorithmes cryptographiques et de protocoles sécurisés pour l'obtention des certificats permet de garantir l'identité de la personne qui a demandé un certificat sur la base de sa clé publique.

Toutefois, un certificat ne garantit pas qu'un message reçu a été signé par le propriétaire de la clé privée associée à la clé publique et utilisée pour la signature du message reçu. Plus précisément, un certificat ne garantit pas qu'une clé privée utilisée pour la signature d'un message n'a pas été dérobée ou utilisée à l'insu de son propriétaire.

Stockée sur un ordinateur personnel, la clé privée est susceptible d'être dérobée ou modifiée ou utilisée à

l'insu de son propriétaire par un tiers malveillant, par exemple par l'intermédiaire d'un virus ou d'un cheval de Troie. Pour éviter ce risque, des matériels spécifiques, tels que des cartes à mémoire associées à un lecteur de carte, ont été développés pour mémoriser notamment les clés privées ; un risque demeure toutefois lorsque la clé privée est lue dans la carte et transmise à un programme de signature présent dans l'ordinateur personnel. Pour limiter encore ce risque, des cartes à microprocesseur ont été développées, qui mémorisent non seulement la clé privée, mais également le procédé de signature utilisant la dite clé privée, de sorte que la clé privée n'est jamais accessible directement depuis l'extérieur, par exemple sur une borne d'entrée / sortie de la carte.

Ainsi, certains des matériels et des procédés actuels permettent le renforcement voire la suppression des risques de vol ou de l'usage d'une clé privée à l'insu de son propriétaire.

Toutefois, un tiers distant, qui a accès seulement à un certificat associé à la clé privée, ne sait pas estimer le risque qu'il prend en acceptant la signature électronique d'un utilisateur distant. Ceci limite bien sûr le degré de confiance qu'un tiers peut avoir dans un certificat numérique ou dans un message signé reçu.

L'invention a pour but de résoudre ce problème en proposant un procédé de production d'un certificat et un certificat associé contenant des informations permettant à un tiers qui reçoit un message signé d'estimer la probabilité pour que l'émetteur de la transaction soit bien le propriétaire authentique de la clé privée utilisée pour la signature.

Pour cela l'invention propose un procédé de production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble de données pour produire un certificat numérique.

Selon l'invention, le procédé est caractérisé en ce que les données numériques comprennent également des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée.

Les données identifiant les moyens de génération de la clé privée pourront par exemple comprendre des données identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée.

Les données identifiant les moyens de mémorisation de la clé privée pourront quant à eux comprendre des données identifiant :

- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée.

Enfin, les données identifiant les moyens de signature pourront par exemple comprendre des données identifiant :

- un procédé de signature utilisant la clé privée,
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

Les données identifiant un matériel ou un support de mémorisation comprennent par exemple :

- une référence identifiant le dit matériel ou le dit support de mémorisation et / ou
- une identification d'un fabricant du dit matériel ou du dit support de mémorisation et / ou
- une indication d'un niveau de sécurité du dit matériel ou du dit support de mémorisation défini selon une norme ISO15408 datée du 01/12/1999.

Les données identifiant un procédé comprennent :

- une référence identifiant le dit procédé et / ou
- une identification d'un inventeur du dit procédé et / ou
- une indication d'un niveau de sécurité du dit procédé selon la norme ISO 15408.

Les données identifiant un lieu comprennent :

- une identification du dit lieu et / ou
- une indication d'un niveau de sécurité du dit lieu selon la norme ISO 15408.

L'invention concerne également un certificat numérique comprenant :

- une clé publique,
- des données identifiant un propriétaire de la clé publique et d'une clé privée associée, et
- des données identifiant des moyens de génération de

la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la dite clé privée.

Dans un mode de réalisation préférée le certificat est de type X509 selon une norme Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks datée de Mars 2000 de l'International Telecomunication Union. Dans le certificat X509, un ensemble de champs prédéfinis et libres sont utilisés pour mémoriser les données numériques identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée et / ou
- un procédé de signature utilisant la clé privée et / ou
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

L'invention concerne également un procédé d'utilisation d'un certificat numérique tel que décrit ci-dessus, comprenant les étapes suivantes consistant à :

- recevoir un message signé avec une clé privée,
- lire, dans le certificat numérique, des données identifiant des moyens de génération de la clé privée

et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée,

- en déduire une probabilité pour que la dite clé privée ait été utilisée par un propriétaire légitime de ladite clé privée,
- en fonction de la dite probabilité, accepter ou refuser le message électronique.

On peut par exemple choisir d'accepter un message uniquement si la probabilité pour que la dite clé ait été utilisée par son propriétaire légitime est supérieur à une valeur prédéfinie VB. La valeur prédéfinie est choisie en fonction du niveau de sécurité souhaité pour une transaction. On pourra par exemple choisir une valeur prédéfinie proportionnelle aux enjeux financiers liés à une transaction.

On peut aussi choisir de :

- accepter le message si la probabilité est supérieure à une première valeur VB1,
- demander une confirmation de la transaction si la probabilité est comprise entre la première valeur VB1 et une deuxième valeur VB2 inférieure à la première, et
- refuser le message si la probabilité est inférieure à la deuxième valeur.

Pour estimer la probabilité pour que la clé privée ait été utilisée par son propriétaire légitime, on utilise les informations relatives à la clé secrète présentes dans le certificat numérique.

Dans un exemple, les informations présentes dans le certificat et relatives à la clé privée indiquent que la clé privée a été générée et mémorisée dans une carte à microprocesseur qui mémorise également un procédé de

signature. Les informations relatives à la clé privée indiquent également que la génération de la clé, sa mémorisation et la mémorisation du procédé de signature ont été réalisés au sein même de l'usine qui a fabriqué la carte, usine possédant un niveau de certification (en terme de sécurité) maximal. Dans ce cas, un tiers qui consulte le dit certificat sait que la probabilité est maximale (et supérieure à la valeur prédéfinie) pour que la clé privée ait été utilisée par son propriétaire légitime et il peut en déduire avec quasi-certitude l'identité de l'émetteur d'une transaction signée qu'il a reçue.

Dans un autre exemple, les informations présentes dans le certificat et relatives à la clé privée indiquent que la clé privée a été générée dans un point de vente de matériel informatique, et que la clé privée et le procédé de signature sont mémorisés sur un disque dur d'un ordinateur personnel. Dans ce cas, un tiers qui consulte le dit certificat sait que la probabilité est forte pour que la clé privée ait pu être subtilisée ou utilisée à l'insu de son propriétaire. Il peut en déduire que l'identité de l'émetteur d'une transaction signée qu'il a reçue n'est pas certaine et en conséquence, décider de refuser la transaction pour éviter un risque.

REVENDICATIONS

1. Procédé de production d'un certificat numérique au cours duquel une autorité de certification regroupe, dans un ensemble de données, une clé publique et des données numériques comprenant des données identifiant le propriétaire de la dite clé publique et d'une clé privée associée, puis signe l'ensemble de données pour produire un certificat numérique,

le procédé étant caractérisé en ce que les données numériques comprennent également des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée.

2. Procédé selon la revendication 1, dans lequel les données identifiant les moyens de génération de la clé privée comprennent des données identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée.

3. Procédé selon la revendication 1 ou 2, dans lequel les données identifiant les moyens de mémorisation de la clé privée comprennent des données identifiant :

- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou

- un support de mémorisation sur lequel est mémorisée la clé privée.

4. Procédé selon l'une des revendications 1 à 3, dans lequel les données identifiant les moyens de signature comprennent des données identifiant :
- un procédé de signature utilisant la clé privée,
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

5. Procédé selon l'une des revendications 2 à 4, dans lequel les données identifiant un matériel ou un support de mémorisation comprennent :
- une référence identifiant le dit matériel ou le dit support de mémorisation et / ou
- une identification d'un fabricant du dit matériel ou du dit support de mémorisation et / ou
- une indication d'un niveau de sécurité du dit matériel ou du dit support de mémorisation défini selon une norme ISO15408.

6. Procédé selon l'une des revendications 2 à 5, dans lequel les données identifiant un procédé comprennent :
- une référence identifiant le dit procédé et / ou
- une identification d'un inventeur du dit procédé et / ou
- une indication d'un niveau de sécurité du dit procédé selon la norme ISO 15408.

7. Procédé selon l'une des revendications 2 à 6, dans lequel les données identifiant un lieu comprennent :
- une identification du dit lieu et / ou
- une indication d'un niveau de sécurité du dit lieu selon la norme ISO 15408.

8. Certificat numérique comprenant :

- une clé publique,
- des données identifiant un propriétaire de la clé publique et d'une clé privée associée, et
- des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la dite clé privée.

9. Certificat selon la revendication 8, de type X509 selon une norme Information technology - Open Systems Interconnection - The Directory : Public-key and attribute certificate frameworks datée de Mars 2000 de l'International Telecomunication Union , dans lequel un ensemble de champs prédéfinis et libres sont utilisés pour mémoriser les données numériques identifiant :

- un procédé de génération de la clé privée et / ou
- un matériel sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de génération de la clé privée et / ou
- un procédé de mémorisation de la clé privée sur un support et / ou
- un matériel sur lequel est mis en œuvre du procédé de mémorisation de la clé privée et / ou
- un lieu sur lequel est mis en œuvre le procédé de mémorisation de la clé privée et / ou
- un support de mémorisation sur lequel est mémorisée la clé privée et / ou
- un procédé de signature utilisant la clé privée et / ou
- un support de mémorisation sur lequel est mémorisé le dit procédé de signature.

10. Procédé d'utilisation d'un certificat numérique selon l'une des revendications 8 ou 9, comprenant les étapes suivantes consistant à :

- recevoir un message signé avec une clé privée,
- lire, dans le certificat numérique, des données identifiant des moyens de génération de la clé privée et / ou des moyens de mémorisation de la clé privée sur un support et / ou des moyens de signature avec la clé privée,
- en déduire une probabilité pour que la dite clé privée ait été utilisée par un propriétaire légitime de ladite clé privée,
- en fonction de la dite probabilité, accepter ou refuser le message électronique.

11. Procédé selon la revendication 10, dans lequel le message est accepté uniquement si la probabilité pour que la dite clé ait été utilisée par son propriétaire légitime est supérieur à une valeur prédéfinie.

12. Procédé selon la revendication 10, dans lequel :
- on accepte un message si la probabilité est supérieure à une première valeur (VB1),
- on demande une confirmation du dit message si la probabilité est comprise entre la première valeur (VB1) et une deuxième valeur (VB2) inférieure à la première valeur, et
- on refuse le message si la probabilité est inférieure à la deuxième valeur (VB2).

reçue le 19/03/04

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg - 75800 Paris Cedex 08

Pour vous informer : INPI DIRECT
N° Indigo 0 825 83 85 87
0,15 € TTC/mn
Télécopie : 33 (0)1 53 04 52 65

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 210103

Vos références pour ce dossier *(facultatif)*	017096
N° D'ENREGISTREMENT NATIONAL	0401976

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de production d'un certificat numérique, et certificat numérique associé, et procédé d'utilisation d'un tel certificat numérique.

LE(S) DEMANDEUR(S) :

GEMPLUS
Avenue du Pic de Bertagne
Parc d'Activités de Gemenos
13420 GEMENOS
France

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		GIRARD
Prénoms		Pierre
Adresse	Rue	CABINET BALLOT 9 rue Claude Chappe
	Code postal et ville	57070 METZ
Société d'appartenance *(facultatif)*		GEMPLUS
2 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

LECLAIRE Jean-Louis 93.4009.

CABINET BALLOT
CONSEILS EN PROPRIÉTÉ INDUSTRIELLE
9, rue Claude Chappe
Technopôle Metz 2000
57070 METZ

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.